Copyright © 2016 International Journal of Cyber Criminology (IJCC) – Publisher & Editor-in-Chief – K. Jaishankar ISSN: 0973-5089
July – December 2016. Vol. 10 (2): 110–126. DOI: 10.5281/zenodo.163398/ IJCC is a Diamond Open Access (Authors / Readers No Pay Journal).

Sexual Extortion of Children in Cyberspace

Kemal Veli AÇAR[1]
Turkish National Police, Turkey

Abstract

This paper examines Sexual Extortion of Children in Cyberspace (SECC), which has gained notoriety despite the fact that it has recently emerged, and is also considered one of the most significant online threats to children in 2015 Internet Organized Crime Threat Assessment (IOCTA) report of Europol. After the characteristics and frequently-observed modus operandi of SECC are described, the points of differentiation and overlap between SECC and other related concepts about online child sexual abuse will be examined. Then, the constituent elements of SECC will be identified and explained in detail; later, possible prevention strategies and research areas will be discussed individually for each one. However, whether SECC should be defined as a separate criminal act and the legal conditions of punishment in the current criminal law systems are completely ignored.

Keywords: Online Child Sexual Abuse, Sexual Extortion, Sextortion, Policing, Raising Awareness, Cyber crime.

Introduction

Anonymity and speed provided by cyber space have made it easier to meet new people at an unprecedented rate. Traditional web forums and chat rooms such as IRC, which became hugely popular in the beginning of Internet Age, lost their dominance to social networking sites such as Twitter and Facebook (Peris et al., 2002; Ellison, 2007). Recently though, mobile dating applications such as Tinder (Roeffen, 2015) have started to enjoy a great popularity. In addition, some platforms such as online gaming sites (Cole & Griffiths, 2007) have made it easier to meet new people indirectly despite the fact that they do not specifically aim at the socialization of users. While such tools, applications and websites lose their popularity over time, they do not completely disappear. Therefore, the new means of socialization in cyberspace cause an expansion in the amount of communication channels available online.

Young people, who embrace technological advances, electronic gadgets, and the emerging social networking applications most rapidly, have become the ones who use such means of socialization most frequently as well (Madden, Lenhart, Duggan, Cortesi, & Gasser, 2013; Lenhart, Purcell, Smith, & Zickuhr, 2010). Furthermore, thanks to Voice-over Internet Protocol (VoIP) applications, they are able to engage in video chat shortly

[1] Superintendent, Unit Manager, Technical & Operational Support Unit, Department of Cybercrime, Turkish National Police, Turkey. Email: kemalveli.acar@egm.gov.tr

after they meet on the communication channels mentioned above, even carrying the online friendships to real life in case of geographical proximity. However, this vast domain of social networking creates a wide attack surface for cyber threats targeting children (Livingstone & Smith, 2014). As a result, the Internet has become a place where potential victims can be "hunted" with the help of the diverse channels of online communication.

Unfortunately, it is only when a shocking news makes it to the headlines does the public learn about new online threats to children. In this context, the suicide of Amanda Todd, a 15-year-old Canadian girl, was the first sensational incident that brought up the Sexual Extortion of Children in Cyberspace. Having recorded a webcam chat where Amanda showed her breasts, a Dutch adult threatened her to broadcast the video online unless she performs 3 more "shows". When the abuser carried out his threat, the victim changed her residence and school, upon which the abuser set up fake social media profiles of the victim in a special effort to make sure that her new friends learn about the incident (Victims of Violence, n.d.).

This article examines Sexual Extortion of Children in Cyberspace (SECC), which has gained notoriety despite the fact that it has recently emerged, and is also considered one of the most significant online threats to children in 2015 (Europol, 2015). Visibility of this offence is very low to law enforcement agencies because a relatively small number of victims and abusers are reported or caught. Therefore, it is difficult to reach a significant and reliable amount of samples to conduct a scientific research. However, gaining a deep insight into SECC and developing efficient prevention strategies on the basis of such insights without waiting for establishment of a measurable and comparable group of victims or abusers would undisputedly provide practical benefits. For this reason, it has become necessary to make some assumptions on the behaviors of victims and abusers. Created by basing on the real life cases, various reports and academic studies on the issue, such assumptions will be hopefully tested by further research.

In this respect, after the characteristics and frequently-observed modus operandi of SECC are described, the points of differentiation and overlap between SECC and other related concepts about online child sexual abuse will be examined. Then, the constituent elements of SECC will be identified and explained in detail, and possible prevention strategies and research areas will be discussed individually for each one. However, whether SECC should be defined as a separate criminal act and the legal conditions of punishment in the current criminal law systems of countries is not within the scope of this article.

Defining Sexual Extortion of Children in Cyberspace

A specific type of sexual abuse associated with workplaces, conventional sexual extortion, despite being the eponym of SECC, is a concept that differs greatly from SECC in some essential respects to be mentioned later in this article. Sexual extortion is characterized by senior managers sexually exploiting their inferiors or candidate employees by threats based on career processes such as denial to employment, dismissal from the job, or denial of the opportunity of promotion (Baker, 1994). However, the term gained a new and unexpected sense by the beginning of the Internet age. Despite the fact that every SECC incident varies in many respects from each other, such acts are committed as follows in simple terms: Once the abuser obtains the sexual materials of the child, the abuser threatens the child with misusing them unless the child complies with his/her demands.

According to the typology of child pornography offending made by Krone, SECC is classified under the category of online grooming (Krone, 2004). On the other hand, Kopecky defines SECC as one of the manipulative techniques used in various processes such as cyber bullying, cyber harassment, and cyber grooming (Kopecký, 2014; personal communication, January 1, 2016). Recently, Interagency Working Group, which was formed by members from several international institutions and non-governmental organizations, published Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Under the section of solicitation of children for sexual purposes, SECC is defined as "the blackmailing of a person with the help of self-generated images of that person in order to extort sexual favors, money, or other benefits from her/him under the threat of sharing the material beyond the consent of the depicted person" (Interagency Working Group, 2016)

These definitions and categorizations of SECC mostly considered it a part or method of other types of online offences against children such as grooming and sexting. Nomenclature and definition of online threats to children is still a hot topic that exceeds the purpose and scope of this study. For this reason, the author will make a quick comparison with SECC through the widely accepted definitions of the relevant concepts without engaging in further conceptual discussions. Later, the author will propose a definitional method which includes every instance of SECC.

Child abuse materials have gained an unprecedented prevalence, reaching incredible numbers due to rapid spread of the Internet and the advance of technological devices (Taylor & Quayle, 2003). In fact, visual materials obtained by abusers through SECC are also child pornography, and such materials might sometimes be put into circulation online. Moreover, according to some views, when such materials are considered new or rare, they facilitate admission of new members or raise the reputation of the existing ones in online groups formed by abusers (Virtual Global Taskforce, 2015). In this respect, SECC can be considered a new method of producing child abuse materials without a doubt. On the other hand, Online Grooming is characterized by establishment of friendship between the abuser and the child for the purpose of physical abuse. Manipulative techniques such as posing as the child's fellow friend, flattery or spoiling the child with gifts are used to lay the groundwork for physical contact with the child (O'Connell, 2003). If the abuser brings the online abuse to the physical world or attempts to do so by means of threatening the victim, the SECC turns into online grooming.

Sexting is an umbrella term that is defined by sending sexual content such as text messages and images by phones or other means of communication. The concept of self-produced child pornography, which can be considered a sub-branch of sexting, stands for obscene images taken and sent to others voluntarily by minors. Such materials are generally used for cyber bullying and revenge porn for the purpose of disgracing the victim in the eyes of his/her friends and family (Leary, 2009; Siegle, 2010). Vast majority of child abuse materials in SECC are made by the victim, and obtained by the abuser through various means. In this respect, it is fair to argue that sexting, which is already getting more prevalence in child abuse materials (Wolak, Finkelhor, & Mitchell, 2012), is also a substantial providing element of SECC. Another threat mentioned in IOCTA 2015 report of Europol, live streaming child abuse, also bears some similarities to SECC with regard to the intensive use of VoIP technologies. In this heinous offence, the live images of sexually abusing the child can be viewed on VoIP in return for a fee (The European

Financial Coalition against Commercial Sexual Exploitation of Children Online, 2014). Considering that a "live sexual show" is generally demanded in SECC, it would be reasonable to assume that sextortionists are potential customers of live streaming child abuse. Lastly, it is possible to consider within the definition of cyber stalking the abuser's attempts to subjugate the child by repeated threats, and broadcasting the images of the child online or sending them to the child's family or friends if the child refuses to comply (Goodno, 2007).

SECC has very close ties with other types of online offences against children. In order to differentiate it from them, the focus should be put on the elements which only and all SECC acts have. This approach will be more beneficial for understanding the threat better and developing more effective prevention strategies than forming a one-size-fits-all definition. In this respect, 3 recurrent characteristics always emerge despite several little differences between the individual cases. Not bringing the interaction and abuse between the abuser and the victim to the physical world (Cyberspace); Possession of obscene images of the child by the abuser regardless of the means of production and acquisition (Possession); Forcing the child to perform certain acts based on the possession of such images (Extortion). Coexistence of all these three elements constitutes the offence of SECC. Absence of any of these elements either prevents the criminality completely or constitutes an offence other than SECC.

Prior Case Studies

The only research that directly deals with SECC was made by Kopecky who studied 15 incidents reported in Czech Republic from 2012 to 2015. Kopecky states that SECC takes place in 5 stages, namely Get in Touch with the Child, Manipulation through Compliments, Verification of the Victim's Real Identity, Intimacy Intensifying, and Multistage Blackmail (Kopecký, 2014). Although this study succeeded in explaining the SECC incidents which involve the use of manipulative techniques of online grooming, it fails to cover other methods such as hacking the victim's computer or accidental/irresponsible sharing in online environments.

Due to severe underreporting, it is very difficult to figure out the true scope of SECC. However, findings of the National Centre for Missing and Exploited Children (NCMEC), which is a US-based non-governmental organization, might be a good start to form an opinion about the victims, abusers, and the methods and threats used in the offending process. Forty-one percent of the 801 reports delivered to them from October 2013 to June 2015 indicate the use of multiple online platforms in the commission of offence. The communication between the abuser and victim usually begins on social networking sites. And later, it continues on instant messaging and video chat platforms for obtaining the sexual images of child. Furthermore, it is observed that 78% of incidents feature victimization of girls and 12% feature victimization of boys. While the majority of reports (76%) involve demand for generally more obscene images from victims, 6% involve demand for money, and 6% involve demand for sexual intercourse (NCMEC, 2015).

Kopecky et al. analyzed the contents of communications between the abusers and children on online platforms to figure out the subjects of threats that the victims are exposed to (Kopecký, Hejsek, & Kusá, 2015). According to the study, threatening to broadcast the images online was the most frequent threat while sending the images to the friends and family was in the second place. In this respect, the results of the study confirm the findings of NCMEC. Of the reports delivered to NCMEC, 71% involve threatening to broadcast obscene images online, and 29% involve threatening to show the images to family members and friends.

A recent study published by US-based non-Governmental organization, Brookings Institution also confirms some of the findings by NCMEC and contribute additional information about offenders. Of all the sextortion cases, every single prosecuted perpetrator was male (Wittes, Poplin, Jurecic, & Spera, 2016). Although this study also covers offenders who target adult victims, anecdotal evidence support this finding for SECC as well. There hasn't been a known case of SECC in which a female offender is involved.

According to the NCMEC's study, the primary purpose of the abusers on SECC is to produce child abuse materials, while it is unclear whether the materials produced are solely for self-satisfaction or additionally used for commercial purposes. Kopecky believes that most abusers victimize children for self-satisfaction (Kopecky, personal communication, January 5, 2016) but commercial sexual extortion is also a known area of concern for law enforcement agencies (The European Financial Coalition against Commercial Sexual Exploitation of Children Online, 2014) Operation Strikeback, which was initiated after the suicide of a 17-year-old Scottish teenager named Daniel Perry, is a publicized example of commercial SECC. A gang of 58 Philippine citizens lured hundreds of victims to engage sexually explicit behaviors before webcam. After surreptitiously recording the chats, they threatened them by broadcasting their obscene images unless the gang members are paid 1000 dollars on average (UNODC, 2015). Most victims were middle-aged males but minors like Daniel Perry were victimized as well. This sensational operation in April 2014 is also significant for pointing out the differences of sexual extortion targeting adults from SECC. SECC involves individual offenders making mostly sexual demands from minors. On the other hand, sexual extortion targeting adults majorly involve offenders acting under an organized criminal structure victimizing especially middle age males to make monetary demands (Trendmicro, 2015; Joyce, 2012). In this regard, sexual extortion of adults in cyberspace has closer ties with online dating romance scam than SECC (Whitty, 2015).

It's not also clear why most offenders prefer additional child abuse images from victims, instead of physical abuse. At first sight, the small percentage of sexual intercourse demands might be related to geographical proximity between the victim and abuser. A long distance to victim can prevent the SECC offender to become online groomer or rapist. However, all the subjects and their victims in Kopecky's study were located in Czech Republic and none of the offenders even attempted to physical abuse (Kopecky, personal communication, January 5, 2016).

Elements of Sexual Extortion of Children in Cyberspace

Unlike Kopecky who studied how SECC takes place, the author will focus on the conditions that should be present to make SECC possible to be committed. As mentioned before, in doing so, it will be possible to differentiate SECC from other online threats to children. Furthermore, analyzing constituent elements of this offence will definitely help to understand specific attributes of the interaction between the victim and the abuser for each stage. Hopefully, developing more effective combating and prevention strategies will follow this comprehensive analysis.

Cyberspace

Although it seems so obvious for an online threat to children, cyberspace is the main element which differentiates SECC from online grooming. Therefore, it deserves short but concise mention. If abuser demands a physical meeting with victim in the extortion phase, this will transform the offence into online grooming. Unless such demand is carried out in an explicit or implicit way, the act remains within the boundaries of SECC.

Possession

In conventional sexual extortion, abusers do not try to find a trump card that will ensure compliance of the victim. In superior - inferior and employer - job applicant relationships, the abuser sustains his threats with the advantage of career superiority that he already holds against the victim (Murr, 2005). In other words, the imbalance of power that is present from the beginning of the relationship is exploited by the offender. SECC lacks this kind of a power imbalance in the beginning of the relationship between the abuser and the child. On the contrary, it is fair to say that the child is more powerful in the beginning of the interaction. Because, the child does not become a victim of SECC unless his/her obscene images get into possession of the abuser, no matter how much time the child spends online and how many dangerous people he/she contacts.

The imbalance of power that is established by superiority of physical force in bullying and by anonymity of offender(s) and variability of attacks in cyber bullying (Butler, Kift, & Campbell, 2009), is established in SECC when child abuse materials are possessed by the abuser. Since the element of possession creates an imbalance of power between the parties and gives an incredible advantage to the abuser in reinforcing extortion threats, it can be easily considered the most critical element of SECC.

In addition, possession is the element that brings the sexuality to SECC. While the things that the abuser demands from the victim in conventional sexual extortion make the act sexual, the obscene nature of the child's images possessed by the abuser in SECC causes the offence to be a sexual one. In this respect, even if the abuser makes monetary demands from the child in the extortion phase, the sexuality of SECC does not change as long as the obscene images of victim are used as leverage.

The most frequent method of obtaining the materials in SECC is that the abuser establishes a relationship by gradually increasing the confidence of the child, and using this relationship to persuade him/her to perform obscene acts before webcam (The European Financial Coalition against Commercial Sexual Exploitation of Children Online, 2014). For this reason, various manipulation techniques used for influencing, persuading and directing the victim in the process of online grooming are heavily adopted by extortionists as well. In addition, it is frequently observed that abusers use methods of social engineering, which is also defined as hacking humans (Mann, 2012; Hadnagy, 2010), in order to engage the children in certain actions by manipulating psychological weaknesses of them. From 2011 to 2013, Jordan James Kirby obtained obscene photographs of women and young girls by introducing himself as the owner of a modeling agency on social media platforms. Kirby blackmailed victims by using the images sent by them in the hope of becoming a famous model. During the relationships, he also used his photographs that feature him posing with a great amount of money in order to convince his targets (FBI, 2015). Using the manipulative methods of social engineering and online grooming depends on specific characteristics of the abuser and the victim. Therefore, time period, form and intensity of such tactics widely varies between each case.

Despite being used relatively less frequently, there are also other ways of possessing the obscene materials without earning the trust of the victim, or even without contacting him/her. Already willing to show and express themselves, young people tend to use the plenty of fast visual sharing possibilities irresponsibly, making themselves vulnerable to various online risks (Livingstone, 2008). In an exemplary case, a 16-year-old girl accidentally uploads to her social media profile an obscene photograph of her and deletes it in a short time, only to see that the photograph was downloaded by one of her schoolmates, who threatened her with broadcasting the photograph online unless the girl refuses to take more obscene photographs and send them to him (Wolak & Finkelhor, 2011). With the increasing ability of and incentive attitude towards uploading personal pictures to online environments, it is reasonable to expect that accidental/irresponsible sharing of youth will continue to be an important risk factor for SECC.

Lastly, it is also possible to obtain child abuse materials by hacking the information systems used by the child and taking over the control of cameras embedded in mobile or desktop devices. In 2010, US citizen Patrick Connolly was convicted of hacking into girls' computers and forced them into making pornographic materials of themselves (Edwards, 2010). However, it is observed that hacking is adopted exceptionally even though it is a more convenient way compared to unintentional uploads that require a plenty of luck to catch and time-consuming manipulation methods of online grooming and social engineering. Brookings Institution's paper also supports this anecdotal evidence. Hacking was only involved in nine percent of SECC cases. This can be attributed to abusers' lack of knowledge about information and communication systems compared to other cyber criminals.

Extortion

Extortion is made by using the methods of threat or intimidation to gain pecuniary or non-pecuniary benefit. Exposing embarrassing information was a method already used to make it easier to subjugate people before the digital age (Lindgren, 1993). Furthermore, many aspects of conventional extortion also apply to SECC. For instance, the fact that the cost of execution of the threat would be very low for the extortionist increases the credibility of threats significantly (Levmore & Porat, 2014). The possibility of easily and rapidly broadcasting the possessed materials online or sending them to the victim's close circle of friends and family without disclosing the true identity of the abuser enhances the influence of his/her threats. In addition, lack of communication between the past and potential victims causes uncertainty as to whether the abuser actually executes his threats to victims in case of non-compliance. A similar version of this uncertainty arises in conventional extortion as the number of victims increases (Konrad & Skaperdas, 1997).

At the stage of extortion, there is not any tool that can enable the victim to counteract the effective threats of the abuser. Even to neutralize or reverse the imbalance of power between him/her and the abuser is almost impossible. In the face of demands that are reinforced with threats that can be executed easily, but still are not certain to be carried out, the victim primarily has 3 options: Complying with the demands of the abuser, refusing to comply with the demands of the abuser and informing the family or official authorities, and refusing to comply with the demands of the abuser and not mentioning this matter to anyone.

Complying with the demands of the abuser and refusing to comply with them and informing the family or official authorities are two closely related options. Child's compliance with the demands of the abuser is generally attributable to the fear of different types of bullying such as slut shaming for girls and gay-bashing for boys. This makes the secret relationship of abuse preferable to possible secondary victimizations in the social life of the child. In some cases, the extent of embarrassment and abasement that might arise from disclosure of images to the child's close circle disturbs the child so much and leaves him/her in such a sense of despair, acts of self-harm extending to suicide are observed (Rigby & Slee, 1999).

Ignoring the threats of the abuser, cutting all connections with him, and not telling the incident to anyone is another possible reaction of victims at the stage of extortion. In the incidents witnessed by the author, majority of victims resort to this option rather than compliance, self-harm, and informing the others. Whether the dominant psychological factor that directs children to act this way is ignorance, a sense of hope mixed with fear, or an unfounded courage is uncertain and needs to be studied. On the other hand, abusers generally start looking for their next victim instead of executing their threats, and keep the images of victims on their personal archives rather than spreading them, or sometimes share these images with other abusers (Kopecky, personal communication, January 5, 2016).

Implications for Research and Practice

As stated earlier, coexistence of 3 elements enables the commission of SECC. Disrupting only one of these elements creates an effective obstacle for abusers in the way of offending. Therefore, it is feasible and possible to develop specific prevention strategies and direct further research around each element.

Cyberspace

According to the routine activity theory, combination of motivated offenders with suitable targets in the absence of capable guardians gives rise to opportunities for offences (Cohen & Felson, 1979). Despite some views against applying this theory to cyber crime (Yar, 2005), it is considered that the theory might provide guidance in determining possible measures regarding the cyberspace element in development of strategies for prevention of SECC (Marcum, Higgins, & Ricketts, 2010). In this respect, prevention of the encounters between the potential abusers (motivated offenders) and children (suitable targets) by enhancing the effectiveness of the existing capable guardians in cyberspace or creating new capable guardians is the first thing that comes to mind. However, it is not that easy to get satisfying results in practice.

Currently, service providers (SPs) report a SECC incident on their platforms to relevant law enforcement units directly or indirectly. However, the fact that victimized children generally refrain from reporting to SPs for socio-psychological reasons and that third persons rarely witness the private communication between the victim and the abuser causes SECC to be underreported. Except for user reporting, the measures that can be taken by SPs for preventing SECC or making it more visible have a limited field of application and rate of success (Livingstone, Ólafsson, & Staksrud, 2011; Quayle & Taylor, 2011; Cano, Fernández, & Alani, 2014; Pendar, 2007).

Parents can be capable guardians on cyberspace by monitoring the online activities of their children through installing certain applications on connected devices of their children, thus identifying a threat when it arises (Dombrowski, LeMasney, Ahia, & Dickson, 2004). The applications and software called monitoring tools allow surveillance of children on both computers and mobile devices. However, effectiveness of these solutions is closely related to the knowledge of children on information and communication technologies. It also requires great deal of time and effort to track the daily online activities for parents. Consequently, it is considered that establishing a healthy communication channel with children, talking to them about the online threats that he/she may encounter, and creating a family environment where the child can tell his/her problems comfortably would be more helpful than the technological measures (Shin, 2015).

In cyberspace, law enforcement can assume the role of capable guardians to deter motivated offenders. Undercover agents may provide the information of an incident or possible abuser by sting operations (Wolak, Finkelhor, & Mitchell, 2009; Mitchell, Wolak, & Finkelhor, 2005). However, while the encounters between the victim and the abuser took place in a limited number of places such as chat rooms and a few popular instant messaging applications in the first years of the Internet, such encounters may now occur on hundreds of environments such as social media websites, gaming sites, and mobile applications. Conducting sting operations to deter motivated offenders in such an extensive domain requires a large amount of human resources and time. Considering that law enforcement resources are already insufficient even for the victim identification in child abuse materials, it does not seem suitable to allocate these limited resources to a preventive measure with little or no potential of success.

To sum it up, in the context of developing a crime prevention strategy, it is almost impossible to keep out children entirely from cyberspace and would do more harm than good even if it is done. On the other hand, keeping them clear of online threats with the efforts of service providers, parents and law enforcement requires constant attention, time and money, and does not guarantee success. For cyberspace element of SECC, it is not feasible to develop more effective preventive measures at the moment.

Possession

Compared to the possible measures of cyberspace element, enhancing the knowledge of children about the benefits and risks brought by cyberspace and thus, making them capable of protecting themselves is more feasible and less costly than keeping their devices and online activities constantly under control.

To emphasize again, the abuser's possession of the sexual images of a child constitutes the backbone of SECC. So much so that it is almost impossible for a child that does not produce his/her sexual images to be a victim of this offence. Therefore, raising the awareness of a child stands out for avoidance of future victimization. Thus, turning into a conscious user of the Internet and devices, the child would be aware of the possibility that any personal information and image that he/she shares online can be used maliciously. Law enforcement agencies in several countries are well aware of this fact, and have conducted raising awareness programs to prevent the online victimization of children.

In the safer surfing program organized by UK Metropolitan Police, there is an interactive part that involves an officer posing as a child, trying to arrange a meeting with the children on an online chat room (Davidson & Martellozzo, 2004). Again in the UK, the projects ThinkUKnow organized by Child Exploitation and Online Protection Centre

(CEOP), and "Getting to know IT all" conducted by Childnet International in collaboration with Virtual Global Taskforce, Microsoft and MSN also aimed to raise awareness on safe use of devices and the Internet among young people (Wishart, Andrews, & Yee, 2005; Davidson, Lorenz, Grove-Hills, & Martellozo, 2009). The program "keeping ourselves safe" conducted by the New Zealand police organization for an effective combat with sexual abuse of children was developed to cover safe use of devices and the Internet from the age of 8-10 (Briggs & Hawkins, 1994; Butterfield, 2002). Also, the NetSmartz initiative that is constituted by NCMEC, Internet Crimes against Children Task Force, and Boys and Girls of America in the United States developed special programs for 3 groups of children, younger elementary school children, older elementary school children and middle and high school students (Kerlikowske & Wilson, 2007). Apart from these publicized examples, awareness raising activities such as organizing seminars in schools, broadcasting public service announcements on mass media, distributing brochures on basic Internet security are carried out through regional or individual initiatives in many different countries.

Understandably, every country evaluates a needs analysis and prioritization based on their respective socio-demographic structure, education system, and the level of crime that is reflected to statistics or perceived by the society. Therefore, preparation and implementation processes of programs, identification of target groups, and the methods of transferring information to such groups vary among different countries, and even across a given country. However, as far as SECC is concerned, online environments, manipulative methods and threats that take part in the commission of offence are almost universal and independent of the geographical location of parties involved. This gives rise to the opinion that similar preventive measures can be developed in a global scale. Therefore, the pros and cons of the programs that have been carried out in different parts of the world, and the lessons learned about such programs regarding both the executives of such programs and children should be identified. Thus, standardized awareness-raising programs can be developed against SECC. With minor modifications, these programs can be integrated in socio-demographic structure of any country. In doing so, countries would be able to start implementing the standardized programs by adding some socio-cultural adaptations rather than designing awareness-raising campaigns from scratch. Considering the widely-accepted importance of awareness-raising programs on cyber crimes, this type of global combating strategy can pioneer similar activities in other domains. This kind of standardization might be conducted simultaneously worldwide under the leadership of Interpol or United Nations, or it might be started with the initiative of a limited number of countries that are party to the European Council's Convention on Cybercrime.

Extortion

If the child feels the social support he/she would receive when the offence is reported or the abuser executes his threat; that would outweigh the negative reactions, and the child would refuse to comply with the abuser more easily. It has been shown that young people get over bullying and other traumatic incidents with less psychological harm and experience milder effects of traumatic stress disorder in the presence of perceived or actual social support (Sapouna & Wolke, 2013; Rothon, Head, Klineberg, & Stansfeld, 2011; Haden, Scarpa, Jones, & Ollendick, 2007). For this reason, the positive perception that the family and the circle of friends would support the victim of SECC does not only relieve the symptoms of post-traumatic stress disorder after victimization but it also reduces the perceived fear factor of the abuser's threats for the victim. Thus, fewer children will feel obliged to comply with the demands of the abusers.

In an interesting case witnessed by the author, an adult male introduces himself as a girl to a young boy, and makes him masturbate before the webcam. When the abuser blackmails the boy, he tells the incident to his elder brother who threatens to find and kill the abuser if he publishes the obscene images of his brother online. Given a taste of his own medicine, the abuser terminates his contact with the child and does not execute his threats. This incident, which can also be explained by the privileged position of boys in the Turkish social structure, is an exceptional example of the victim's neutralization of threats when he finds himself in a supportive environment. However, if it was a girl or a child with homosexual tendencies involved in a similar incident, the possibility of seeking help or getting support from the close circle would be significantly lower.

Making small modifications in the contents of preventive measures that are considered successful in fighting bullying, the message that child should be supported after victimization can be delivered in short term. In long term, developing socio-psychological dynamics to relieve the fear of children to experience a secondary victimization, establishing a more supportive social environment, and facilitating pursuit of professional, social and legal support might eliminate the imbalance of power at the stage of extortion significantly. Due to persistence of victim blaming in sexual offences for a long time, implementation of these suggestions which may look easy on paper should be extended over years and realized by an arduous process that requires a rigorous implementation.

Whether SECC is a new and specific type of online child sexual abuse or a small part of current offending is of great importance in developing tailor-made solutions. For this reason, detailed interviews with convicted offenders might present more reliable findings on how decision-making process of offenders works at this stage. Demanding additional child abuse material instead of an actual physical abuse, even in case of close distance to victim, needs to be studied in particular. The abuser might demand extra "shows" from victim since the live interaction between each other is less risky or sexually more stimulating than physical abuse. Alternatively, it is possible that total control over victim makes the abuser feel psychologically superior and this feeling of superiority might satisfy him/her so much that physical sexual abuse becomes needless or undesirable.

Another area that also needs special attention is why abusers rarely executes their threats and usually moves to next victim. It is important to know whether offenders consider their threats intimidating or bluffs. Possibly, abusers opt to abandon executing the threat after analyzing the cost and benefit of the action (Shavell, 1993). Publishing the images of the child online or sending them to the family or friends of the child would pose the risk of making his anonymous activities noticeable to law enforcement, thereby increasing the cost of execution of the threat. Except for psychological reasons such as holding a grudge against the victim or taking pleasure in harassing him/her, the abuser does not benefit from executing his threat. Refusal of compliance indicates that the victim does not acknowledge the power of the abuser. Execution of the threat would not restore the imbalance of power in favor of the abuser that was balanced upon child's refusal to comply and so it would not cause the child to submit to the abuser. From the perspective of the abuser, since execution would not bring a power similar to the one he gained after possession of obscene materials, execution of the threat might become completely futile.

It is also observed that some abusers victimize hundreds of children. Therefore, the forensic examination of these prolific offenders' conversations with victims might give a comprehensive account of why some children comply with the demands and others do not. Anecdotal evidence suggests that refusal of the child to comply with the threats of the abuser can be considered a passive but effective method. Nevertheless, extra care must be taken for policymaking based on similar results. If future studies confirm the best option for the victim is "do not comply, terminate contact and forget about it", it might give rise to unintentional but harmful outcomes in the long run in combating this offence. Above all, this suggestion would make an already underreported offence even less visible. Abusers would run a much smaller risk of being caught even if they target more children in the end. Additionally, abusers will definitely adopt their modus operandi in regard to general behavioral change of possible victims. They might start executing their threats against some of the children for the sake of earning reputation in order to increase the perceived power and intimidation of their threats. Consequently, it is crucial to understand the dynamic nature between abuser and victim before considering any change on policy making.

Conclusion

Previously defined as a superior or an employer making sexual demands from employees or candidate employees by career-related threats, the concept of sexual extortion has gained a new definition and form with the Internet and become one of the primary methods of sexual abuse of children in cyberspace. Fundamentally, Sexual Extortion of Children in Cyberspace (SECC) is based on the acts of an abuser to demand benefits from a victimized child with the threat of publishing obscene visual materials of the child online or sending them to the family or friends of the child. Although it is closely related to child pornography, self-produced child pornography, sexting, online grooming and online harassment, SECC has its own distinctive characteristics.

The distinctive characteristics can be called cyberspace, possession, and extortion, and SECC occurs when all of them are present. What is meant by cyberspace is that the communication between the parties and the abuse take place in cyberspace and are not brought to physical environment. The element of possession represents the abuser's acquisition of obscene visual materials of the child. While the imbalance of power in conventional sexual extortion is already present between the victim and the extortionist, it emerges only when the abuser gains the possession of obscene images of the child in SECC. Moreover, while what makes the offence sexual in conventional sexual extortion is the abuser's demands, it is the content of the child's images in SECC. The most important element of SECC, possession is generally ensured by using manipulative communication techniques of online grooming and persuading the child to produce obscene materials. Albeit infrequently, images that are accidentally/irresponsibly uploaded by the child, or that are obtained by hacking the computer/account of the child might also be used. In the stage of extortion, abuser influences the child to do certain actions primarily by threatening to send the obscene materials in his possession to the family or friends of the child. Usually, the demands are of sexual nature such as masturbating or undressing. However, except for physical meeting, monetary or other demands might be made at this stage.

Prevention strategies and further research for SECC can be classified, evaluated and developed around the constituent elements of this offence. Regarding cyberspace, preventive measures require excessive and constant allocation of money, time, and labor by service providers, parents, and law enforcement. They have a limited field of application and a low chance of success, especially compared to their costs. In addition, no matter how many risky friendships a child may engage in online, he/she will not be a victim of SECC unless his/her sexual images are possessed by an abuser. In this respect, raising awareness among children for safe Internet and device use would be less costly and more effective than preventive measures that might be introduced with regard to the cyberspace. Since the SECC is almost not influenced at all by geographical locations of the abuser and the victim, and the socio-cultural structures that they are subject to; it seems possible to create a common global standard on awareness-raising programs for prevention of possession. At the stage of extortion, the balance of power is already disturbed in favor of the abuser, and the child has little chance to neutralize or reverse the resulting imbalance. The potential reaction from the family and friends in the event of abuser's execution of his threats causes the child to be overwhelmed by an intensive sense of embarrassment and despair, and eventually to comply with the demands of the abuser. In this respect, society should be supportive in order to reduce the fear of the child to suffer secondary victimization. In short term, by small modifications to anti-bullying programs, a victim of SECC can be prevented from becoming a victim of bullying as well. In long term, strategies extended over years should be developed to change for the better the society's established perception and attitudes towards victimized children.

The fact that abusers and victims are scattered to a lot of countries and the offences are underreported constitutes a negative impact on measurements and assessments of SECC in scientific terms. As a result, there needs further research on the behavior patterns of offenders and victims. Demanding additional child abuse material instead of an actual physical abuse, even in case of close distance to victim, needs to be studied in particular. Additionally, why some children comply with the demands of abuser and others do not is another important area of concern. It is hoped that assumptions on SECC based on personal experiences and publicized examples will be tested by comprehensive interviews with convicted offenders of SECC, and examination the digital evidences of communication with victims.

References

Baker, C. N. (1994). Sexual Extortion: Criminalizing Quid Pro Quo Sexual Harassment. *Law & Ineq.*, *13*, 213.

Briggs, F., & Hawkins, R. M. (1994). Follow-up data on the effectiveness of New Zealand's national school based child protection program. *Child abuse & neglect*, *18*(8), 635-643.

Butler, D., Kift, S., & Campbell, M. (2009). Cyber bullying in schools and the law: Is there an effective means of addressing the power imbalance. *eLaw J.*, *16*, 84.

Butterfield, L. (2002). NetSafe: the New Zealand model for Internet (ICT) safety education. Retrieved from http://workspace.unpan.org/sites/internet/documents/S6NZ02%20NetSafe%20%20The%20New%20Zealand%20Model%20for%20Internet%20(ICT)%20Safety%20Education.pdf.

Cano, A. E., Fernandez, M., & Alani, H. (2014, November). Detecting Child Grooming Behaviour Patterns on Social Media. In *International Conference on*

Social Informatics (pp. 412-427). Springer International Publishing.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, *44* (August), 588-608.

Cole, H., & Griffiths, M. D. (2007). Social interactions in massively multiplayer online role-playing gamers. *CyberPsychology & Behavior*, *10*(4), 575-583.

Davidson, J. C., & Martellozzo, E. (2004). Educating children about sexual abuse and evaluating the Metropolitan Police Safer Surfing Programme. (Project Report) London, U.K. : Metropolitan Police.

Davidson, J., Martellozzo, E., & Lorenz, M. (2009). Evaluation of CEOP ThinkUKnow internet safety programme and exploration of young people's internet safety knowledge. Other. Centre for Abuse & Trauma Studies and Kingston University. Retrieved from http://www.cats-rp.org.uk/pdf%20files/Internet%20safety%20report%204-2010.pdf.

Dombrowski, S. C., LeMasney, J. W., Ahia, C. E., & Dickson, S. A. (2004). Protecting Children From Online Sexual Predators: Technological, Psychoeducational, and Legal Considerations. *Professional Psychology: Research and Practice*, *35*(1), 65.

Edwards, A. (2010, June 18). *Judge calls child exploiter a 'narcissistic demon,' hands down 30-year sentence.* Retrieved from http://articles.orlandosentinel.com/2010-06-18/news/os-orlando-child-exploitation-20100618_1_sentence-patrick-connolly-victims-lives.

Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer‐Mediated Communication*, *13*(1), 210-230.

Europol. (2015). *The Internet Organised Crime Threat Assessment (IOCTA) 2015.* Retrieved from https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web_2015.pdf

Goodno, N. (2007). Cyberstalking, a new crime: Evaluating the effectiveness of current state and federal laws. *Missouri Law Review*, *72*.

Haden, S. C., Scarpa, A., Jones, R. T., & Ollendick, T. H. (2007). Posttraumatic stress disorder symptoms and injury: The moderating role of perceived social support and coping for young adults. *Personality and Individual Differences*, *42*(7), 1187-1198.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.

Interagency Working Group. (2016). *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.* Retrieved from www.interpol.int/Media/Files/News-Media-releases/2016/Terminology-Guidelines.

Joyce, M. (2012). Video Chat Extortion and Sexual Abuse. *형사정책연구소식*, *122*(단일호), 20-32.

Kerlikowske, R. G., & Wilson, M. (2007). NetSmartz: a comprehensive approach to internet safety and awareness. *Police Chief*, *74*(4), 46.

Konrad, K. A., & Skaperdas, S. (1997). Credible threats in extortion. *Journal of Economic Behavior & Organization*, *33*(1), 23-39.

Kopecký, K., Hejsek, L., Kusá, J., Marešová, H., & Řeřichová, V. (2015). Specifics of children communication and online aggressors within the online assaults on children (analysis of selected utterances). In *SGEM2015 Conference Proceedings* (pp. 195-202).

Kopecký, K. (2014). Stručný úvod do problematiky online vydírání českých dětí se zaměřením na tzv. sextortion. *Pediatrie pro Praxi*, *15*(6), 352-354.

Krone, T. (2004). *A typology of online child pornography offending*. Canberra, Australia: Australian Institute of Criminology.

Leary, M. G. (2009). Sexting or Self-Produced Child-Pornography-The Dialog Continues-Structured Prosecutorial Discretion within a Multidisciplinary Response. *Va. J. Soc. Pol'y & L.*, *17*, 486.

Lenhart, A., Purcell, K., Smith, A., & Zickuhr, K. (2010). Social Media & Mobile Internet Use among Teens and Young Adults. Millennials. *Pew internet & American life project*.

Levmore, S., & Porat, A. (2014). Credible threats. Coase-Sandor Working Paper Series in Law and Economics. Retrieved from http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2378&context=law_and_economics.

Lindgren, J. (1993). The theory, history, and practice of the bribery-extortion distinction. *University of Pennsylvania Law Review*, *141*(5), 1695-1740.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New media & society*, *10*(3), 393-411.

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry*, *55*(6), 635-654.

Livingstone, S., Ólafsson, K., & Staksrud, E. (2011). Social networking, age and privacy. EU Kids Online, London, UK. Retrieved from http://eprints.lse.ac.uk/35849/1/Social%20networking%2C%20age%20and%20privacy%20%28LSERO.pdf.

Madden, M., Lenhart, A., Duggan, M., Cortesi, S., & Gasser, U. (2013). *Teens and technology 2013*. Washington, DC: Pew Internet & American Life Project.

Mann, M. I. (2012). *Hacking the human: social engineering techniques and security countermeasures*. Gower Publishing, Ltd.

Marcum, C. D., Higgins, G. E., & Ricketts, M. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal justice review*. 35(4), 412-437.

Mitchell, K. J., Wolak, J., & Finkelhor, D. (2005). Police posing as juveniles online to catch sex offenders: Is it working?. *Sexual Abuse: A Journal of Research and Treatment*, *17*(3), 241-267.

Murr, H. S. (2005). Continuing Expansive Pressure to Hold Employers Strictly Liable for Supervisory Sexual Extortion: An Alternative Approach Based on Reasonableness, The. *UC Davis L. Rev.*, *39*, 529.

O'Connell, R. (2003). A typology of child cybersexploitation and online grooming practices. Retrieved from http://image.guardian.co.uk/sys-files/Society/documents/2003/07/17/Groomingreport.pdf.

Pendar, N. (2007, September). Toward Spotting the Pedophile Telling victim from predator in text chats. In *ICSC* (Vol. 7, pp. 235-241).

Peris, R., Gimeno, M. A., Pinazo, D., Ortet, G., Carrero, V., Sanchiz, M., & Ibanez, I. (2002). Online chat rooms: Virtual spaces of interaction for socially oriented people. *CyberPsychology & Behavior*, *5*(1), 43-51.

Quayle, E., & Taylor, M. (2011). Social networking as a nexus for engagement and exploitation of young people. *Information Security Technical Report*, *16*(2), 44-50.

Rigby, K., & Slee, P. (1999). Suicidal ideation among adolescent school children, involvement in bully—victim problems, and perceived social support. *Suicide and life-threatening behavior*, *29*(2), 119-130.

Roeffen, C. (2015). Mobile dating: Romance is just a swipe away Tinders' Romantic and sexual interactions. Utrecht Faculty of Humanities Theses (Pre-master project). Retrieved from http://dspace.library.uu.nl/bitstream/handle/1874/320142/BA-%20werkstuk%20Caro%20Roeffen%204127994%20Augustus%202014.pdf?sequence=2.

Rothon, C., Head, J., Klineberg, E., & Stansfeld, S. (2011). Can social support protect bullied adolescents from adverse outcomes? A prospective study on the effects of bullying on the educational achievement and mental health of adolescents at secondary schools in East London. *Journal of adolescence*, *34*(3), 579-588.

Sapouna, M., & Wolke, D. (2013). Resilience to bullying victimization: The role of individual, family and peer characteristics. *Child abuse & neglect*, *37*(11), 997-1006.

Shavell, S. (1993). An economic analysis of threats and their illegality: Blackmail, extortion, and robbery. *University of Pennsylvania Law Review*, *141*(5), 1877-1903.

Shin, W. (2015). Parental socialization of children's Internet use: A qualitative approach. *New media & society*, *17*(5), 649-665.

Siegle, D. (2010). Cyberbullying and Sexting: Technology Abuses of the 21st Century. *Gifted child today*, *33*(2), 14.

Taylor, M., & Quayle, E. (2003). *Child pornography: An internet crime*. Brunner-Routledge, Hove.

The European Financial Coalition against Commercial Sexual Exploitation of Children Online. (2014). *Strategic Assessment of Commercial Sexual Exploitation of Children Online*. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/efc_strategic_assessment_2014.pdf.

The National Center for Missing and Exploited Children. (2015). *Sextortion*. Retrieved from http://www.missingkids.com/Sextortion.

Trendmicro. (2015). *Sextortion in the far east*. Retrieved from http://www.trendmicro.com.ru/cloud-content/us/pdfs/security-intelligence/white-papers/wp-sextortion-in-the-far-east.pdf.

United Nations Office on Drug and Crime. (2015). *Operation Strikeback*. Retrieved from http://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/phl/operation_strikeback.html.

U.S. Federal Bureau of Investigation. (2015). *Facebook Predator Sentenced to 29 Years in Prison in for Child Pornography and Sexual Extortion Offenses* [Press Release]. Retrieved from https://www.fbi.gov/sacramento/press-releases/2015/facebook-predator-sentenced-to-29-years-in-prison-in-for-child-pornography-and-sexual-extortion-offenses.

Victims of Violence. (n.d.). *Crime on the Internet*. Retrieved from http://www.victimsofviolence.on.ca/research-library/crime-on-the-internet/#sexual-extortion.

Virtual Global Taskforce. (2015). *Child Sexual Exploitation Environmental Scan*. Retrieved from https://www.europol.europa.eu/sites/default/files/publications/vgt_cse_public_version_final.pdf.

Whitty, M. T. (2015). Anatomy of the online dating romance scam. *Security Journal*, 28(4), 443-455.

Wishart, J., Andrews, J., & Yee, W. C. (2005). Evaluation of the 'Getting to Know IT All' presentation as delivered in UK schools during November 2005. *Bristol: University of Bristol.*

Wittes, B., Poplin, C., Jurecic, Q., & Spera C. (2016). *Sextortion: Cybersecurity, teenagers, and remote sexual assault*. Retrieved from http://www.brookings.edu/~/media/Research/Files/Reports/2016/05/sextortion/sextortion1.pdf?la=en.

Wolak, J., & Finkelhor, D. (2011). Sexting: A typology. Retrieved from http://www.unh.edu/ccrc/pdf/CV231_Sexting%20Typology%20Bulletin_4-6-11_revised.pdf.

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2009). Trends in Arrests of "Online Predators".

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2012). Trends in Arrests for Child Pornography Production: The Third National Juvenile Online Victimization Study (NJOV ‐ 3).

Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427.